

John Mansfield, OSB No. 055390
john@harrisbricken.com
Megan Vaniman, OSB No. 124845
megan@harrisbricken.com
HARRIS BRICKEN
511 SE 11th Ave., Ste. 201
Portland, OR 97214
503-207-7313
Attorneys for Plaintiff

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON
PORTLAND DIVISION**

DALLAS BUYERS CLUB, LLC,

Plaintiff,

v.

JOHN HUSZAR,

Defendant.

Case No.: 3:15-cv-00907-AC

**DECLARATION OF JOHN MANSFIELD
IN SUPPORT OF PLAINTIFF'S
RESPONSE IN OPPOSITION TO
DEFENDANT'S MOTION FOR
SUMMARY JUDGMENT**

I, John Mansfield, hereby declare as follows:

1. I am attorney with the law firm of Harris Bricken, and am the attorney representing Plaintiff in this action.

2. Attached as Exhibit 1 is a true copy of the expert report prepared by forensic consultant Stephen M. Bunting, the owner of Bunting Digital Forensics, LLC, with his Curriculum Vitae attached.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge, and I understand that it is made for use as evidence in court.

DATED: April 9, 2018, in Portland, Oregon.

s/ John Mansfield

John Mansfield
Declarant

EXHIBIT 1



Bunting Digital Forensics, LLC
33579 Blue Heron Drive
Lewes, DE 19958
Phone: +1.302.260.2633
www.BuntingDigitalForensics.us

Expert Report – Testing of GuardaLey LTD's MaverickEye UB (MEU) Copyright Infringement Detection System

Prepared by: Stephen M. Bunting, EnCE, CCFT
CEO / Senior Forensic Consultant
Bunting Digital Forensics, LLC

DECLARATION OF STEPHEN M. BUNTING

I, STEPHEN M. BUNTING, DO HEREBY DECLARE:

1. My name is Stephen Michael Bunting. I am over the age of twenty-one (21), and I am competent to make this Declaration. I make this Declaration voluntarily and the facts stated herein are based on my personal knowledge and information.

2. I currently work as Director of Services for SUMURI, LLC and as independent forensic consultant as owner of Bunting Digital Forensics, LLC. Prior to that, I was a police officer from 1980 until 2009 with the University of Delaware Police from which I retired as a Captain. During the last ten years with the University of Delaware Police, I was in charge of the digital forensics and cyber investigations unit, that I founded. From 2009 until early 2013, I was a Senior Forensic Consultant with Forward Discovery, LLC, which in late 2012 was acquired by Alvarez and Marsal (NY) where I was a manager in the digital forensics division. I founded Bunting Digital Forensics, LLC in early 2013.

3. I have taken hundreds of hours of training in digital forensics, network forensics, and cyber investigations. I have provided training in the same topic areas, from beginner to expert levels, to members of various local, state, and federal law enforcement agencies and private sector examiners. I have trained like personnel internationally in over twenty-one (21) different countries. I have provided training, as either a part-time employee or contractor, for Guidance Software, Magnet Forensics, MicroSystemation, A.B., Organization of American States, and the U.S. Department of State Anti-Terrorism Assistance Program (Cyber Division). I have developed digital forensic or cyber training programs for several government and private entities.

4. I hold several industry-related certifications. I was the recipient of the 2002 Guidance Software Certified Examiner Award of Excellence for receiving the test score on my certification examinations. Among my varied certifications I am an EnCase Certified Examiner EnCE (Guidance Software), an AccessData Certified Examiner (ACE), Certified Computer Forensics Technician (HTCN), and a Certified XRY Instructor.

5. I am the principle author of *EnCase Computer Forensics - The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition*, the co-author *Mastering Windows Network Forensics and Investigation*, the author of *EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 2nd Edition*, the co-author *Mastering Windows Network Forensics and Investigation 2nd Edition*, the author of *EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition* (all published by Wiley).

6. I have written numerous articles in the field of digital forensics over my career. Most recently I published two articles regarding spoliation examinations in which several peer-to-peer cases on which I have consulted were referenced in a hypothetical context:

Forensic Analysis of Spoliation and Other Discovery Violations - Part 2 of a 2-Part Series - Windows Examinations - eForensics Magazine - December 2016

Forensic Analysis of Spoliation and Other Discovery Violations - Part 1 of 2-Part Series - Macintosh Examinations - eForensics Magazine - October 2016

7. I have testified as a fact and expert witness numerous times in the field of computer forensics before state and federal courts in Delaware and New Jersey. I have submitted affidavits, as an expert in digital forensics, on many matters in several states, including Delaware, Georgia, and South Carolina.

8. No court has ever refused nor has any attorney ever challenged to accept my testimony on the basis that I was not an expert or not qualified in the field of computer forensics.

9. As a digital forensics examiner I have acquired and examined hundreds of computer systems and mobile devices for various local, state, and federal agencies, in addition to scores of private clients. The types of cases or examinations include: homicide, child-exploitation, fraud, Medicaid fraud, unlawful intrusion into computer systems (hacking), intellectual property theft, research fraud, email forgery, criminal impersonation, forgery, sexual harassment, peer-to-peer, and spoliation. I have acquired computer systems of many types, including servers, virtual servers, desktops, and laptops. I have acquired hundreds of mobile devices (feature phones and smart phones), both logically and physically. I also have acquired smart phones using JTAG and chip-off techniques, both of which require disassembly and working with the printed circuit boards inside a smart phone.

10. I have considerable experience with network-related cases, such as unlawful intrusions and peer-to-peer cases. I have investigated or provided digital forensics support to several unlawful intrusion incidents in both a law enforcement and a private sector capacity.

11. As a police officer I received specialized training in conducting peer-to-peer investigations by S.A. Flint Waters with the Wyoming Internet Crimes Against Children (ICAC) Task Force. S.A. Waters developed the Wyoming Toolkit, a customized version of Phex, a peer-to-peer client on the Gnutella network. I participated with members of the State of Delaware ICAC in this training program and afterwards in a task force conducting peer-to-peer investigations. Using the Wyoming Toolkit, we searched for child sexual exploitation images and movies on the peer-to-peer networks. When images were found, the software identified offending computers by their IP addresses^{Note 1}.

^{Note 1:} A public or internet routable IP address is a router or computer's address on the internet at a specific time. IP addresses uniquely identify a computer, as no two computers can have the same exact public, internet routable, IP address at the same time. If the address is that of a router, the computer typically has a private address

behind the router. In a typical home network, the ISP provides a 'box', which is often both a modem and a router / firewall / DHCP server. The router has a public or internet facing IP address assigned to it. On the back side of the router, several devices (computers, smart phones, etc) are connected using private addresses. Thus several devices in a home network share the public internet routable address assigned to the ISP's box (router). Other computers on the internet, including peer-to-peer software, see and use the public facing IP address assigned to the customer's router. The router routes network traffic for specific devices on the private side or behind the router using a protocol called NAT (Network Address Translation), thus assuring network traffic is sent to the correct computer.

IP addresses, as mentioned, are often time specific. These IP addresses are called dynamic IP addresses. They are assigned for certain periods of time, called leases. There is great variability in how often dynamic IP addresses change, but because they can and do change, the specific time of the offense is necessary to determine which subscriber was assigned a specific IP address at a specific time. ISP's maintain connection logs that record to whom a specific IP address is assigned and exactly when. By contrast, an IP address can be a fixed IP address. Even they can change and, as an investigator, you do not know which type a subscriber has and thus the exact time is always obtained and submitted to an ISP when requesting subscriber information.

The IP addresses hosting the illegal images are parsed by the toolkit using an IP geolocation database by which offending IP's are isolated or filtered to only those within our police jurisdiction. Once offending IP's were found in Delaware, we would request that the Attorney General's office submit subpoenas to the ISP (Internet Service Provider) for specific customer information and address of the offending IP address. As IP addresses are often time-specific, we submitted the exact date / time (along with time zone offset) for the offending IP address. The ISP would return to us the customer or subscriber information (name, address, account information,

etc.) for the ISP in question. We would investigate further and obtain a search warrant for the premises at which the IP was hosted. The search warrant would permit us to seize all media and electronic devices capable of holding digital media, as we did not know specifically which device behind the router was the offending device. The IP address detected by the peer-to-peer software was the public facing internet addressable IP address of the router, which is associated with the subscriber and their residence and not to a specific computer in the residence. Because it was a criminal investigation, we requested that the subscriber not be notified of the subpoena so that digital evidence would not be destroyed. Thus, in nearly all cases, the offending subscribers were surprised by the execution of the search warrant. In all the times that we did so, not once did the IP address lead to an innocent person's residence. Rather, we always found evidence therein of child sexual exploitation media on the computer system(s) therein.

12. I have found that the Wyoming Toolkit was a most reliable tool for identifying the IP addresses for peer-to-peer clients that were hosting child sexual exploiting images and video.

13. In my experience, the IP address's subscriber, or a family member thereof, is likely the offending party.

14. I have been involved in a case where the owner of the computer and charged party was professing his innocence, claiming someone else must have used his wireless network, citing a neighbor who reportedly engages in photography of a questionable nature. However, the evidence on his computer suggests otherwise. The software used by the investigators detected the name and version of the peer-to-peer software client involved, which happened to match the one found on his machine. Further, the same exact images detected by the investigative software were found on his machine. His claims were without merit and in direct contradiction to the overwhelming digital evidence found on his computer.

15. Unsecured wireless routers in homes used to be commonplace 15 years ago. In recent years, however, Internet Service Providers (ISP's) have undertaken great effort to provide and deploy secured wireless systems. Most "internet interface boxes" (combination modem / router / firewall / DHCP server) are preconfigured to operate with WPA2 security with a complex password already set. These devices are secure out of the box with strong encryption and complex passwords that are lengthy alpha numeric passphrases. Thus, valid claims of compromised home wireless systems today are, in my experience, rare compared to 15 years ago.

16. In the past, I have consulted with Computer Forensics, LLC in copyright infringement cases where spoliation was an issue. I'm familiar with the technology that was used in those cases to detect the copyright infringement offenders.

17. I have been retained by Voltage Pictures, LLC to provide digital forensic services and consulting in matters of copyright infringement. In anticipation of potential testimony in that regard, I have undertaken tests of the infringement detection software used, which is MaverickEye UB (MEU). This software and hardware platform is owned and run by GuardaLey, LTD, a German company located in Eggenstein, Germany. The CEO and Senior Developer at GuardaLey is Benjamin Perino.

18. Mr. Perino has written an expert report describing the features and functions of this proprietary software, MaverickEye UB, or MEU, in detail. I have read that report in its entirety.

19. The manner in which MaverickEye works and the manner in which the software that I have used in my law enforcement capacity (Wyoming Toolkit) work to connect a peer-to-peer violation with an IP and subsequently with a subscriber are quite similar. In fact, MaverickEye UB, in my opinion, is much better with greater integrity features. Based on having read Mr. Perino's expert report on the function and features of the MaverickEye UB system, I note that the MaverickEye UB system is better because of the following: The law enforcement software

does not capture or retain any network packets, whereas MEU does. The law enforcement software does not use a WORM drive to store evidence, whereas MEU does. The law enforcement software is not housed or run in an ISO/IEC 270001:2013 compliant datacenter nor does it comply with PCI security specification, whereas MEU does.

20. I constructed and then conducted a test to determine the accuracy of the MaverickEye software as to its ability to detect an infringing party's IP address, identifying metadata (client software and version used by infringer), and identifying the known test files distributed on the torrent network.

21. To test the MaverickEye software, I created four video files, ones I created and owned from my archives. They were short clips of nature scenes, contained no people, and ones I could readily identify on site as being unique and ones I had in fact created. I embedded identifying metadata into these files, specifically my name, a description of the content, the data, and a statement that was placing them into the public domain. I also created MD5 and SHA1 hashes of each of the four files. A hash is an algorithm that produces a value that is best described as an electronic fingerprint. Files that are identical will have the same MD5 each time it is hashed. The slightest change by so little as one bit will produce a dramatically different hash value. Using this method, file integrity can be assured. Using two different hash algorithms eliminates any possible claims of hash value collisions.

22. I configured four different computers each with a different operating system and each with a different bit torrent client software. Bit torrent client software is used to share files over the bit torrent network using the bit torrent protocol. The below matrix, Table 1 below, shows the test configurations:

Computer	Operating System	Bit Torrent Client
----------	------------------	--------------------

Dell Laptop E6510	Linux Ubuntu 16.04 LTS	KTorrent 4.3.1
Dell Laptop E5500	Windows 7 Professional	BitTorrent 7.10
HP Laptop Envy	Windows 10 Enterprise	uTorrent 3.5.1
MacBook Pro 15" 2016 Touch Bar	High Sierra OS X 10.13.2	Transmission 2.9.2

Table 1- The four test computers, their installed operating systems, and their installed bit torrent clients.

23. After configuring the above laptops, I installed and tested the latest version of Wireshark on each laptop. Wireshark is a software tool that captures the network packets that traverse or are transmitted over any particular network interface on the host computer. Thus, it is a means of recording the traffic over the network. I have used Wireshark and its predecessor, Ethereal, for many years in both my law enforcement and private sector careers. I have also trained others to use it.

24. On a fifth machine, not part of the test, I created torrents of the test or known movie files and allowed them to ‘seed,’ which means to share them on the torrent network and make them available for others to download. I took the four torrent files and physically placed them on the four test laptops, one unique file to each laptop. I started Wireshark on each test machine to capture the download and loaded the torrent files in each laptop’s client software. In short order, each torrent file was able to locate the file and download it from the source machine that was initially sharing all four files. In so doing, the client software on each test machine was found to be working as designed. On each test machine, the newly downloaded movie file appeared to be identical to the original known files, as created. Each was found to contain the embedded metadata, including my name. To be absolutely certain the downloaded files were identical to the source files, each file was hashed and the hashes were found to be identical to those hashes the original files. The results are shown below:

Computer	File Name	MD5 Hash Original	MD5 Hash Downloaded onto Test Machines
Dell Laptop E6510	01CanadianGooseHenonNest.m4v	a13a318a02c32b0d1a8e276ae92227d8	a13a318a02c32b0d1a8e276ae92227d8
Dell Laptop E5500	02GeeseHonkingOK.m4v	6cdca839624df3e7c202766964394069	6cdca839624df3e7c202766964394069
HP Laptop Envy	03StripersJumpingOK.m4v	5ae4fbf8a2b73e131e3f8030ad99242c	5ae4fbf8a2b73e131e3f8030ad99242c
MacBook Pro 15" TouchBar	04WinterWetlandsOK.m4v	36c24f6d10c86df4994e435b055d01f9	36c24f6d10c86df4994e435b055d01f9

Table 2 - Test computers, the test or known file shared by each, and their hash values

25. At this point in the test, the only sources for these four files anywhere were the four test machines and the source machine on which they were created. The source machine torrent client (Transmission) was stopped, making the four test machines now the only sources. The HP Laptop and the MacBook Pro was shut down for the first phase of the test, leaving the two Dell laptops the only sources for the first two files in the list. At this point, I provided the four torrent files to Mr. Perino in Germany. He loaded the torrent files onto the MaverickEye UB system so that the system could attempt to locate the known test files on the torrent network, download them, and identify the IP address of the device responsible for distributing the files.

26. For the first phase of the test, the two Dell laptops were behind a firewall / DHCP server / router and would share the same public facing, internet-routable IP address. They could be distinguished by their port number for the connection, as well as by their bit torrent client and version number. The time was synchronized with a time server and the public, internet-routable address was checked and noted.

27. Once I was informed that the MaverickEye system (MEU) had been loaded with the torrent files, I took the third laptop (HP Envy) to another location to use a different network configuration. The laptop was connected to a network at which I had an account and was configured directly with a public internet-routable IP address, such that the IP address of the laptop itself would be exposed directly to the internet. The time was synchronized with a time server and the public, internet-routable address was checked and noted. After running the test for a little more

than an hour, I was informed that the MEU system had detected all three files thus far placed into the torrent network. I shutdown the HP Envy laptop and returned to my original location where the first two laptops were still running the torrent clients.

28. I connected the fourth laptop to the original network, adding a third machine to the public IP address shared by the first two laptops. The fourth laptop was a MacBook Pro and was sharing the fourth file. The time was synchronized with a time server and the public, internet-routable address was checked and noted. Late in the afternoon, I was notified that all four files had been detected by the MEU system and that the test was concluded.

29. Mr. Perino sent me, via email, a copy of the network packet ^{Note 2} captures (PCAP files) and a spreadsheet summarizing the captures. In addition, he sent me copies of the four files that the MEU downloaded based on the torrent files that I send to him.

^{Note 2} – Information sent over a network travels in packets. Each packet contains, among other data, a destination IP address, a destination port, a source IP address, and a source port. Thus, every packet contains what amounts to a delivery address and a return address, to make this somewhat analogous to the postal system by which mail travels. A stream of packets constituting a bit torrent download will often contain thousands of packets, each and every one of them containing source and destination IP addresses. As those packets also contain the file data of the bit torrent file, the source IP address for packets containing the file data itself is demonstrable evidence of the source of the file captured by the MEU system. A bit torrent network shares files on a peer-to-peer basis, meaning the two computers actually connect to each other. Hence the destination and source IP's represent the two computers involved in this file sharing. Further, these packets travel via a TCP protocol, which is a guaranteed delivery system. If a packet sent is not acknowledged as received, it is sent again and again, until it either is acknowledged or times out and fails.

30. For all four files, the MEU system captured the public, internet-routable IP address for the source of the test or known files that I was sharing on the bit torrent network. I knew exactly what the IP addresses were, as I had recorded them before and after the downloads. The IP addresses involved were dynamic IP addresses and thus time sensitive. The ISP's for those IP addresses maintain logs that record which subscriber or user is assigned a particular IP address at a particular time. Had a subpoena been served on either of the two different ISP's used in this test, I would have been correctly identified as the responsible subscriber / user at those exact times for those involved IP addresses.

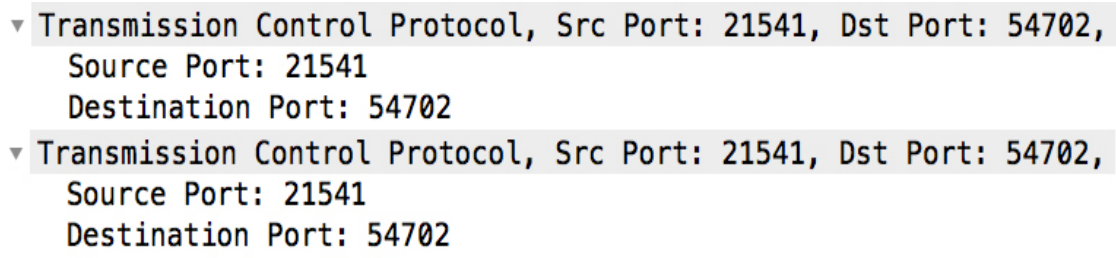
31. Further, the MEU correctly captured the exact name of the bit torrent client and version numbers that were in use by each test computer. This capture is possible because when the MEU first connects to the computer hosting a file to be shared on the bit torrent network, a handshake occurs. Each machine's bit torrent client sends a packet to the other stating, among other things, their peer ID. Part of the peer ID is the name of the bit torrent client followed by its version number. Table 3, below, is a copy of Table 1, above, with an added column at the right showing the Bit Torrent client and version number as it was exchanged in the handshake. You can see that they were correctly identified in each instance.

Computer	Operating System	Bit Torrent Client	Bit Torrent Client Captured by MEU
Dell Laptop E6510	Linux Ubuntu 16.04 LTS	KTorrent 4.3.1	KT4310
Dell Laptop E5500	Windows 7 Professional	BitTorrent 7.10	BT71000
HP Laptop Envy	Windows 10 Enterprise	uTorrent 3.5.1	UT351S
MacBook Pro 15" 2016 Touch Bar	High Sierra OS X 10.13.2	Transmission 2.9.2	TR2920

Table 3 - The 4th column shows the bit torrent client and version number, as captured in the handshake, which

corresponds currently with the installed client.

32. As previously mentioned, the MEU captures the source port number in addition to the source IP address, as they are parts of the ‘address’ of each packet. I confirmed that the port numbers captured by the MEU system were accurate. I did this by spot checking packet captures on both systems. By that, I mean that packets sent and received from a test machine are captured as they are sent. Simultaneously, packets sent and received on the MEU system are likewise captured. As the two machines are connected, peer-to-peer, and the MEU is downloading a file from the test machine, the packets sent and received between the machines are the same packets of data and are being captured simultaneously. Thus, one can examine packets from both machines and can identify them as one and the same. I did this with several packets and this confirms positively that the MEU is accurately reporting the source IP address and other metadata (port numbers, client name, & client version). While making these packet comparisons, I examined the TCP (Transmission Control Protocol) layer of the packets, wherein the port numbers are found and noted that the port numbers are being correctly reported. Figure 1, below, shows the TCP layer information. The top one is from a packet captured on the MEU system, showing the Destination Port for this packet as 54702. The bottom one is from a packet captured on the Windows 10 test laptop (HP Envy). The Destination Port for this packet is also 54702.



▼ Transmission Control Protocol, Src Port: 21541, Dst Port: 54702,
Source Port: 21541
Destination Port: 54702

▼ Transmission Control Protocol, Src Port: 21541, Dst Port: 54702,
Source Port: 21541
Destination Port: 54702

Figure 1 - TCP layers from MEU on top and Windows 10 test machine on bottom. Port numbers match and are being correctly reported by MEU

They are identical and should be for the connection to have been successful. Packets are sent back and forth during a file sharing exchange, regardless of which party is downloading. In this case, the MEU is requesting a segment of the file that is being shared by this machine and identifies it by an index number. The Windows 10 test laptop (HP Envy) machine is using port 54702 for its client (UTorrent) to share files. So, when the MEU sends the request to the Windows 10 test machine, the destination port is 54702. When the Windows 10 test machine sends a packet to the MEU, the Windows 10 machine then becomes the source for the packet and thus the port would be listed as the source port. Thus, the MEU network packet captures are correctly reporting the port on the computer hosting the shared file that is also being identified by its IP address. As the MEU system is obtaining the port information from the network packets and, since the packets are reporting correctly (matching on both sides of the transmission), the summary report from Mr. Perino is listing port 54702 for this particular download is, as to be expected, correct and accurate.

33. Whenever the MEU was connected to my torrent clients to download from them, never did I see it offer any portion of the file to share. At all times it listed it as 0% available when using the inspector to look at connected peers. At one point after the regular test was concluded, I allowed one test machine to download all four files so they could be shared and subsequently detected by the MEU again, this time via a VPN. At that point, minimally, those four files were present on the one source machine on my network and also on the MEU, as all four had been detected and downloaded onto the MEU software. Since I was requesting those same files, were the MEU sharing files it has downloading, it would have responded as a normal torrent client would have responded and allowed my client to download them. The MEU did not connect and provide any download to my test laptop that was seeking those four files for download. Rather, they were downloaded only from sources within my local network of test machines. Thus, based

on the observation I made during a test, I agree with Mr. Perino's description of the MaverickEye software in that it only downloads from clients offering files to share and does not share any files in return.

34. To protect my privacy and to preserve the integrity and confidentiality of the MEU system, no IP addresses for those systems are being specified in this declaration nor are any screen captures of those IP addresses by shown.

35. As previously stated, Mr. Perino provided copies of the test or known files that were downloaded from the test machines by the MEU system. I examined those files and, on visual inspection, I identified them as the same files that I had prepared for this test. I looked inside the files and noted that the metadata was still present exactly as I had inserted the data, including my name. Next, I hashed the known or test files provided by Mr. Perino using both MD5 and SHA1 hashing algorithms. I compared the hashes from the MEU download to the hashes in the original set and found them to be identical. Thus, the files downloaded by the MEU from the test machines, via the bit torrent (peer-to-peer) network were identical, bit-for-bit copies of the original source test or known files.

36. I have concluded, based on this test, that the MaverickEye UB (MEU) infringement detection software works and accurately identifies the IP address of the device responsible for sharing of a particular file on the bit torrent network and the exact time of the violation. The MEU connects to the computer hosting a file that is being shared, peer-to-peer (computer-to-computer). The MEU downloads that file or portions of that file. In our test case, it downloaded the entire file from the test machines, as they existed nowhere else. The files downloaded by the MEU from the test machines were identical in all regards. The hash values matched, proving they were bit-for-bit, identical copies. The MEU captures and retains the network packets involved in the file sharing process, as such network packet captures were made and provided to me as part of the test. Those

network packets contain, among other data, the actual data (shared file content) from the machine that is sharing the file, along with the IP address of the computer sharing that data. MEU will, in fact, often capture hundreds or thousands of packets of data, with each and every packet identified by and containing the violator's IP address, bit torrent sharing port, bit torrent client, and bit torrent client version. Each packet captured will contain the exact time that the packet was transmitted. Per Mr. Perino's expert report, MEU's time is being synchronized with an atomic clock for accuracy. The MEU will not capture every file being shared on the bit torrent network, but for those it is configured to monitor and does capture, that data capture will, in my opinion and based on my testing, accurately identify the public facing, internet-routable IP address of the device sharing that file, as well as the exact time the file was shared. Likewise, it will, in my opinion and based on my testing, also identify the port used by the bit torrent client on the internet facing device if not the computer itself, the actual name of the bit torrent, and the version number of that bit torrent software. Furthermore, based on my testing, the MEU performed accurately regardless of the operating system or the torrent client being used.

37. Based on a combination of my testing and of my understanding of the features and function of the MEU system, having read Mr. Perino's expert report on the MEU system, I am of the opinion that it was designed to maintain the accuracy and integrity of the evidence throughout. For example, as per Mr. Perion's export report, the MEU:

- Captures and retains the actual network packets whereby a file is downloaded from a copyright infringement violator. As noted previously each and every one of those packets identifies the source IP address of the violator and the exact time.
- Said captures are stored on a WORM drive. A WORM drive is a Write Once, Read Many drive, meaning once the evidentiary network packets are written to the drive, they cannot be altered, thus maintaining evidentiary integrity.

- WORM drives containing evidence are stored in a vault
- A log is automatically maintained of each copyright infringement violating download that occurs
- Time accuracy is maintained by synchronization with an atomic clock
- MEU is housed in an ISO/IEC 270001:2013 compliant datacenter
- MEU complies with the PCI security specification

38. As to the possibility of the MEU yielding false positive, I have read Mr. Perino's expert report, specifically section B, items 26, 27, 28, and 29, which deal with "TCP/IP Connections cannot be spoofed and cannot yield false positives." I concur with his statements in 26, 27, 28, and 29.

39. With regard to item 26, it is important to understand that the bit torrent protocol is a peer-to-peer file sharing protocol. Peer-to-peer means just that, a computer-to-computer connection. This means that files or portions of files are shared by direct connections between computers. When a direct connection occurs and packets are exchanged, the destination and source IP addresses of the two connected computers are found in the packets that are exchanged. They must be for the connection to be established and the stream of packets containing the file segments to transmit. Each and every packet contains the IP address of the sender and receiver (source and destination) and this goes for every packet involved in the transaction, not just those containing data. The TCP protocol is, as previously mentioned, an assured delivery system in that packets sent must be acknowledged as received. All the traffic associated with that acknowledgement process also must contain the IP addresses of the sender and receiver.

40. With regard to item 27, IP spoofing can be done by an experienced network specialist. Specially crafted network packets can be used to create denial of service attacks, but these packets are small and usually involve repeatedly sending the same small crafted packet over

and over again, creating a flood of messages that results in a denial of service attack. Creating a few small, specially crafted packets that are sent repeatedly is a completely different task than trying to do so for a bit torrent stream, where tens of thousands of packets, mostly all different, are involved.

41. With regard to item 28, Mr. Perino is accurate in his assessment of complexities and enormity of the task that would be involved in trying to do an IP spoof of a bit torrent stream. In a practical sense, a very technically adept person would have to know a victim's IP address. This person would have to physically connect a computer into the same network segment as the intended victim in order to intercept the network traffic involved. Doing so would involve considerable knowledge and skills, in and of itself, and could involve illegal access to a building or ISP network equipment. The person would need to have the file in question on their computer, be sharing it using bit torrent software, and have some software or code capable of or rewriting tens of thousands of bit torrent packets on the fly, as any delay could cause a time-out. While many things are theoretically possible, I am unaware of any such software being available. Such an endeavor would involve tremendous effort and resources. In addition, the person would have to know that a particular file was being monitored for copyright infringement downloading. And finally, such a person would have to have a very strong motivation to undertake such a task and to target a particular person and/or IP address. Considering all that would be involved in such an endeavor, it is so unlikely to occur as to be nearly impossible, as Mr. Perino states.

42. With regard to item 29, often IP spoofing, as described above, is interpreted or confused by many, including Google's search engine, with IP address hiding. If you search for "IP spoofing software," you will find most of the hits will involve VPN (Virtual Private Network) software. VPN software allows the user of a computer to create an encrypted tunnel to a VPN server from which the internet traffic emerges unencrypted. The VPN server's internet facing IP

address also becomes the user's public internet-routable IP address. It acts as a proxy and is your frontend IP or point of presence IP on the internet. All network traffic between the user and the VPN server is encrypted. VPN's are intended for privacy of a user's internet traffic and also for protecting the identity of their IP address. A proxy server is similar in function to a VPN server. The major difference is that there is no encrypted tunnel between the user and the proxy server. The proxy server still serves, however, as the user's frontend IP or point of presence IP on the internet. A proxy server is not as secure as a VPN server because there is no encrypted tunnel. A proxy server is, however, faster than a VPN server because encryption requires time resources to achieve and results in slower network speeds, all other things being equal. If a VPN or a proxy server is used to engage in bit torrent file sharing, the MEU will see the source IP of the infringer as the public facing, internet routable IP address that of the VPN or proxy server, as that is the user's IP address, by proxy. This is not a false positive by any definition. Rather, the MEU is capturing packets that contain the source IP for the file as that of the VPN or proxy. When a VPN or proxy is being used, MEU can only trace the connection to the front-end or public-facing, internet routable IP address, which is accurate to that point. To obtain the IP of the user behind the VPN or proxy who is responsible for download, the VPN or proxy server owner or manager would have to be contacted. If they maintain logs, and many quite intentionally do not, the connection to the source can then be identified through the subpoena process. Because the front-end interface to the MEU used by plaintiff's counsel only has filters for known ISP's (Comcast, Verizon, AT&T, etc), IP addresses for VPN's and Proxy services are not in those filtered groups and will not be visible.

43. With regard to item 29, I conducted a separate test, after concluding the one described above whereby I configured one laptop (MacBook Pro – High Sierra) with a VPN service. With the VPN enabled, I launched Transmission (bit torrent client) and shared all four test

or known files. I noted the public, internet-routable, frontend IP address in use by the test computer. After running this bit torrent configuration overnight using the VPN service, Mr. Perino reported to me that the MEU captured and downloaded the known or test files from the IP address that I had recorded for the computer. It was, as expected, the IP address of the VPN server. Thus a test of the scenario, as described by Mr. Perino in item 29, it absolutely correctly stated and accurate.

44. When a user adds a torrent file for a file that they want to download, the “Trackers” that are included in the torrent file actively work to connect torrent clients that have either all or parts of a requested file with those seeking those files. In doing so, the IP addresses and port numbers, along with other metadata are shared, visible, and otherwise made public within that ‘swarm’ of torrent users. It is by this mechanism of identifying each computer in the swarm by its IP address and port number that computers in the swarm can connect directly to one another and share parts of the file. It is also by this mechanism that MEU system can see the public IP addresses and port numbers of copyright infringers and connect directly with them to download files and capture evidence of copyright infringement. Such a process is akin to going to a coffee shop and asking if anyone in the room has sugar on their table, as you do not. Perhaps you want 6 packets of sugar and you need a packet or two from several tables to get your 6 packets. The conversations that take place during this discovery and sharing process are very much out in the public for all in the coffee shop to hear. There is no expectation of privacy when such a request is made. Anyone in the coffee shop can see who you are and hear what it is that you are requesting. The swarm works much the same way. Once you announce that you want a file, the trackers in that torrent file being asking other users if they have that file, sharing your IP and port, and thereby facilitating the download of segments of the requested file from many users in the swarm. It matters not where the various torrent clients are located, as the internet is global and crosses nearly all country boundaries. In this case, the MEU happens to be in Germany, but could be anywhere. The simple

fact is that if you wish to join a peer-to-peer, file-sharing network, you have to share your IP address and port with those in that public pool of persons doing likewise. You are agreeing to and consenting to allowing others to connect to your computer in order that you can exchange files. As with asking for a packet of sugar in a crowded coffee shop, those in a swarm will hear your request and know who you are by your public routable IP address.

45. In Mr. Perino's expert report, in number 44, he defines what Bitfield is within the context of the bit torrent network. Each shared file is divided into 16 KB segments or blocks and is shared in increments of 16 KB segments. If a file consists of 5,000 segments and a user had 2,500 segments, that user has 50% of the file and would show a Bitfield value of 50%. When I conducted the test, each of the four laptops had one of each of the four files in its entirety (100%) on each of the laptops. The summary report provided by Mr. Perino after the test showed that the MEU system accurately detected that each of the four files had a Bitfield value of 100%, meaning each laptop had the entire test or known file.

46. Attached hereto as Declaration Exhibit 1 is a true and accurate copy of my Curriculum Vitae which truly and accurately represents my relevant employment history, training, experience, certifications, and expert-witness experience.

47. I am paid on an hourly basis by Voltage Pictures, LLC at the rate of \$250 / hour for my digital forensics services.

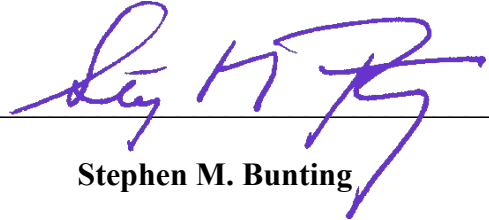
FURTHER DECLARANT SAYETH NAUGHT

DECLARATION

PURSUANT TO 28 U.S.C SS 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed February 2, 2018.

By: _____

A handwritten signature in blue ink, appearing to read "Stephen M. Bunting", is written over a horizontal line. The signature is stylized with a large "S" and "B".

Stephen M. Bunting

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document has been served to all counsel or parties of record who are deemed to have consented to electronic service via the Court's CM/ECF system.

s/ David A. Lowe

LOWE GRAHAM JONES PLLC


701 Fifth Avenue, Suite 4800
Seattle, Washington 98104
206.381.3300 • F: 206.381.3301

EXHIBIT 1

Curriculum Vitae of Stephen Michael Bunting

Bunting Digital Forensics, LLC • 33579 Blue Heron Drive • Lewes, DE 19958
Phone: +1.302.260.2633 • E-Mail: stephenbunting@mac.com

Summary of Experience

Mr. Bunting is an experienced digital forensics examiner and currently works as the Senior Manager of Services for SUMURI, LLC as an independent consultant and as CEO and Senior Forensic Consultant of Bunting Digital Forensics, LLC. Formerly Mr. Bunting was a Manager with Alvarez & Marsal (Sept 2012 to Feb 2013) and prior to that a Senior Forensic Consultant with Forward Discovery (Sept 2009 to Sept 2012). (Alvarez and Marsal acquired Forward Discovery in Sept 2012) His responsibilities with Bunting Digital Forensics, Alvarez & Marsal, and Forward Discovery include:

- Acquisition and forensic examination of digital media using industry standard forensics tools;
- Develop & instruct classes on Windows, Macintosh and Mobile Device Forensics;
- Develop & instruct classes on cyber investigations and related course work;
- Investigative consultation and digital forensics examinations in many areas including spoliation, theft of intellectual property, malware analysis, unlawful access of computer systems, theft of corporate resources, employee misuse of computer systems, Medicaid fraud, and support of various types of criminal investigations (prosecution only - no criminal defense work);
- Consult with clients and develop E-Discovery plans;
- Carry out electronic discovery processing from initial acquisition to final load file;
- Under sub-contract (multiple vendors) to the U.S. Department of State, develop & instruct various cyber-based anti-terrorism courses to international law enforcement agencies.
- Under Bunting Digital Forensics, instruct XRY Foundation, Intermediate, PinPoint, XAMN, and Kiosk Courses. Currently the only contract instructor for MSAB (XRY) in the U.S.
- Under Bunting Digital Forensics, instruct courses for Magnet Forensics as a contract instructor.
- Bunting Digital Forensics is under contract to SUMURI, LLC, whereby Steve Bunting manages the services division of SUMURI.

Mr. Bunting retired from a law enforcement career spanning over three decades, during which he conducted hundreds of examinations of computer systems for the University of Delaware Police as well as federal, state, and local law enforcement and prosecutorial agencies. He is also a trained and experienced forensic video analyst using the [Ocean Systems dTective® and Avid software systems](#). He is a frequent lecturer and instructor on computer forensics, cyber-crime, and incident response.

Mr. Bunting has testified in many trials as a computer forensics expert. He was the recipient of the 2002 Guidance Software Certified Examiner Award of Excellence for receiving the highest

test score on his certification examinations. Among his varied certifications he is an [EnCase Certified Examiner EnCE \(Guidance Software\)](#), an AccessData Certified Examiner (ACE), [Certified Computer Forensics Technician \(HTCN\)](#), and a [Certified XRY Instructor](#).

Mr. Bunting is a retired a police captain, having served in the State of Delaware for over thirty-five years. He created and developed the University of Delaware Police Department's Computer Forensic Lab. He has taught computer forensics for Guidance Software, makers of EnCase, and taught as a Lead Instructor at all course levels, including the Expert Series with particular emphasis on "Internet and Email Examinations" course. He has instructed students in computer forensics on an independent study basis for the [University of Delaware](#) and is an adjunct faculty member of [Goldey-Beacom College](#), teaching computer forensics. He has been a presenter at several seminars and workshops, the author of numerous "white papers", the principle author of [EnCase Computer Forensics - The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition](#), the co-author [Mastering Windows Network Forensics and Investigation](#), the author of [EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 2nd Edition](#), the co-author [Mastering Windows Network Forensics and Investigation 2nd Edition](#), the author of [EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition](#) (all published by Wiley), and maintains a [website](#) for cyber-crime and computer forensics issues.

Recent Consulting Engagements

While Mr. Bunting engages in a significant number of instructional endeavors, a number of consulting engagements have been untaken. Some of those engagements are described below:

Recovered data from an Android phone that had been underwater and was delivered 'in pieces'. Using chip-off technique, all data was fully recovered including data that had been deleted.

Served as an expert for two defendants who were facing spoliation claims. Established that opposing expert had failed to discover settings whereby SMS's messages were forwarded from an iPhone to a MacBook Pro. Opposing expert claimed SMS messages were deleted from the iPhone when in fact they were in the opposing expert's possession on the MacBook Pro. Said deletions were offered as evidence of spoliation. Opposing expert also failed to find over 11,000 AIM Messenger chats that were on the iPhone.

Served as a trusted third-party digital forensic examiner in a Virginia case where a former employee was accused of theft of intellectual property, specifically programming code. Determined that accused party provided fabricated exhibits to examine in the form of a contrived MacBook Pro in which the time had been altered to appear to contain historical data when in fact it was only 3 weeks old.

Conducted digital forensics examinations of computers believed to be involved in a telecommunications fraud in the Middle East region, whereby perpetrators were conducting a multi-million dollar fraud in a balance transfer scheme exploiting a software defect.

Conducts ongoing training and course development for the U.S Department of State's Anti-Terrorism Assistance Program Cyber Division. As such six to eight courses are delivered each year in varying international locations.

Ongoing consultation with a digital forensics firm that specializes in examinations for copyright infringement cases in the motion picture industry involving peer-to-peer clients to download movies and other protected media.

Ongoing consultation with a digital security company in the UAE, providing incident response support services.

Developed a new Macintosh Digital Forensics course for the Delaware State Police Child Predator Task Force. The course is an in-depth program intended for those with significant digital forensics experience. It includes a unique module entitled "Digging Deeper – Research Techniques to Establish User Culpability", which is the first of its kind.

Developed and delivered a virtual course entitled: Cyber Security Investigations: Incident Response for the FedCTE program. The course was developed for virtual delivery using the AvayaLive virtual classroom and first delivered on June 25, 2014.

Provided expert witness services establishing that the plaintiff fabricated an email submitted during discovery in a civil matter. Testified in US District Court (Princeton, NJ) as expert for defense in computer forensics analysis and email analysis in a hearing to dismiss based on fraudulent documents offered into evidence by plaintiff. Specifically, testified that document proffered as an email was in fact fabricated to appear as such. – July 09, 2014. The matter is still under litigation.

As a member of a team, conducted an on-site assessment of a major middle east country's governmental cybercrime unit and digital forensics unit, prepared gap analysis reports, and prepared recommendations for creating ISO 17025 compliant laboratory operations, a modern cybercrime investigation and intelligence gathering unit, as well as country-wide expansion of capabilities for both units.

Assigned as principal leak investigator for a major mobile device manufacturer. Investigated significant intellectual property losses on a global basis.

Conducted a security assessment, as part of a team, of a Caribbean country's government IT infrastructure and made recommendations for securing their systems according to best practices.

Conducted computer forensic examination of all computers from a dental practice in a Medicaid fraud case. Examination involved reconstruction of a dental practice's business transactions spanning several years through analysis of SQL transaction logs from Patterson's *Eaglesoft* dental practice software. The findings in the report submitted substantiated ongoing fraud and induced a guilty plea, resulting in the incarceration of the offending dentist.

Conducted computer forensic examination of over two-dozen laptops belonging to employees of a major brand integrity unit, which investigates and mitigates brand piracy for its parent company. The unit was distributed in six countries and had been accused of various breaches of duty and unlawful acts. The examination took several months to complete and findings documented and substantiated the majority of the allegations, resulting in the dismissal of several employees.

Certifications

Certified XRY Instructor, MSAB (Sweden)	October 2013
Certified ACE AccessData Certified Examiner	April 2011
Certified iPhone Examiner, MSAB	November 2010
Certified XRY Complete Examiner, MSAB	October 2010
Certified LAW PreDiscovery Administrator, LexisNexis	January 2010
Certified LAW PreDiscovery User, LexisNexis	January 2010
Certified Computer Forensic Technician, High Tech Crime Network	September 2001
EnCase Certified Examiner, Guidance Software	April 2002
Certified Cell Phone Examiner, Paraben Corporation,	May 2005
Certified PDA Examiner, Paraben Corporation	May 2005
State of Delaware Council on Police Training Certified Police Officer	April 1975

Employment History

SUMURI, LLC – Camden, DE – Senior Manager of Services – November 2016 to present

- Provide management services for SUMURI's Services Division
- Develop and carry out the business plan for services
- Coordinate services, match resources with service needs, and ensure quality control
- Conduct digital forensic examinations and investigations

Bunting Digital Forensics, LLC – Lewes, DE – CEO & Senior Digital Forensic Consultant – February 2013 to present

- Conduct digital forensics examinations on a variety of media, including mobile devices
- Develop training programs for various cyber related topics
- Deliver training programs as an independent contractor for the Antiterrorism Assistance Program Cyber Division (see NDI below)
- Conduct assessments of digital forensics laboratories, conduct a gap analysis, and recommend a roadmap for improvements leading to accreditation
- Conduct specialized digital forensics examinations in support of Medicaid fraud cases

Microsystemation (MSAB) – Stockholm, Sweden – Contract instructor for XRY training courses – October 2013 to present

Teach XRY Mobile Device Forensic Solutions Courses

Alvarez and Marsal, Washington, DC – Manager, Forensic Technology Services – September 2013 to February 2013

- Develop and deliver a variety of training courses, including Macintosh Forensics, Incident Response, and Advanced Digital Forensics Courses.
- Developed and facilitated a table top training exercise to test and enhance the incident response capabilities of a large web hosting company
- Conduct digital forensic examinations on media associated with compromised systems.
- Interim Management, specifically Principle Leak Investigator for a large telecommunications company experiencing a significant loss of intellectual property.

Forward Discovery, Inc – San Antonio, TX – Senior Forensic Consultant – September 2009 to September 2012

Information security company that provides digital investigation, electronic discovery, vulnerability assessments and training services to corporate and government clients.

- Acquisition and forensic examination of digital media using industry standard forensics tools
- Develop & Instruct classes on Windows, Macintosh and Mobile Device Forensics
- Develop & Instruct classes on Cyber Investigations and related course work
- Investigative consultation in areas including theft of intellectual property, malware analysis, unlawful access of computer systems, theft of corporate resources, employee misuse of computer systems, and support of various types of criminal investigations (prosecution only - no criminal defense work).
- Consult with clients and develop E-Discovery plans
- Carry out electronic discovery processing from initial acquisition to final load file

Network Designs, Inc. – McLean, VA – Senior Instructor ATA Cyber Division as an Independent Contractor – September 2009 to present. On a contract basis to NDI, work as a Senior Instructor supporting the U.S Department of State Anti-Terrorism Assistance Program's Cyber Division, which included the following:

- Develop training modules for new training programs
- Provide advisement, briefings and presentations to foreign law enforcement officers on areas including cyber terrorism and cyber crime
- Provide technical computer investigation training to law enforcement and governmental agencies worldwide. Course taught include: Identification & Seizure of Digital Evidence, Introduction to Digital Forensics & Investigations, Macintosh Forensics, Cell Phone Forensics Consultation, EnCase Software Consultation, Server Incident Response (ADFC), Fundamentals of Network Security, Cyber Unit Management Consultation Proactive Internet Investigations Course, Forensic Equipment Grant Consultation, and Digital Forensic Lab Mentoring and Consulting.

Guidance Software – Pasadena, CA – Part-time Instructor - 2004 - 2005.

- Lead instructor teaching courses at all levels (Beginning to Expert)
- Assisted in course development and review

University of Delaware Police Department – Newark DE – Captain - July 1980 to August 2009.
Principle duties were:

- Computer Forensics Unit
- Accreditation
- Southern Operations

Education

University of Delaware - Computer Applications Certificate – Concentration in Network Environments - August 2004

Wilmington College - Bachelor of Science Applied Professions / Business Management - May 1986

Delaware Technical and Community College - 52 credit hours in the Criminal Justice Program

University of Delaware - Associate in Art - May 1973

Publications

[Forensic Analysis of Spoliation and Other Discovery Violations](#) - Part 2 of a 2-Part Series - Windows Examinations - eForensics Magazine - December 2016

[Forensic Analysis of Spoliation and Other Discovery Violations](#) - Part 1 of a 2-Part Series - Macintosh Examinations - eForensics Magazine - October 2016

[EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide](#), 3rd Edition - author - Wiley - September 2012

[Mastering Windows Network Forensics and Investigation](#) (one of four co-authors) - Wiley - 2012

[EnCase Computer Forensics—The Official EnCE: EnCase Certified Examiner Study Guide](#), 2nd Edition - author - Wiley - November 2007

[Mastering Windows Network Forensics and Investigation](#) (one of two co-authors) - Wiley - April 2007

[Encase Computer Forensics—The Official EnCE: Encase Certified Examiner Study Guide](#) - primary author - Wiley - January 2006

Memberships and Affiliations

[Infragard](#) – secure member of the Wilmington, [Delaware Chapter](#) since June 2004.

[High Technology Crime Investigation Association](#) - member since August 2002.

[High Tech Crime Network](#) - member from September 2001 to date.

[National White Collar Crime Center](#) - designated agency contact person for agency membership in the organization - January 2001 to 2009.

Courses Recently Developed

Chip-off / JTAG Bootcamp – A two-day course intended for stand-alone or to supplement a forensic software course. A pilot was recently delivered in January 2017.

Macintosh Digital Forensics – A new course for delivery by Bunting Digital Forensics to various clients. August 2015.

Cyber Security Investigations: Incident Response – New course development and delivery (part of two-person teams) – course was created for virtually delivery using the AvayaLive virtual classroom, with first delivery on June 25, 2014.

Mastering Macintosh Forensics – Rewrite (part of a four-person team) – Alvarez & Marsal for U.S. Department of State ATA – February 2013 – March 2013

Introduction to Digital Forensics and Investigation - Rewrite (part of two-person team) - U.S. Department of State ATA (Humtech) May 2012 - January 2013

Windows Server Incident Response - New course (part of two-person team) - Organization of American States May 2012 - Sept 2012

Advanced Digital Forensics Consultation (Windows / Linux / Macintosh Server Incident Response), New course (solo assignment) plus developed and built portable server lab -U.S. Department of State ATA - Sept 2011 - March 2012

Mastering Macintosh Forensics - New course (solo assignment) - U.S. Department of State ATA - Jan - June 2011

Languages

Primary language is English, however during last several years have spent considerable time teaching and consulting in Latin American countries through interpreters, during which some Spanish skills have been acquired. Currently have the ability and experience demonstrating, teaching, and using EnCase and XRY software using the Spanish interface.

Teaching and Presentation Experience

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Dec 11-15, 2017, Nigerian MOI in Dubai, UAE.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Nov 27- Dec 1, 2017, Nokesville, VA.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Aug 21-25, 2017, Lansing, MI.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Mar 6-10, 2017, Singapore.

Chip-off Forensics Bootcamp – Sumuri, LLC – January 30, 2017, Dover, DE.

Foundation, Intermediate, XAMN XRY Mobile Phone Forensics – Micro Systemation, A.B. – Oct 24-28, 2016, Nairobi, Kenya.

Introduction to Digital Forensics and Investigation - U.S. Department of State ATA, July 18 - 29, 2016, Shillong, Meghalaya - India.

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – July 6-15, 2016 – Shillong, Meghalaya – India.

Foundation XRY Mobile Phone Forensics – Micro Systemation, A.B. – May 16-17, 2016, U.S. Secret Service National Computer Forensics Institute Hoover, AL.

Foundation and Intermediate XRY Mobile Phone Forensics (private course for 5 members of the Kingdom of Saudi Arabia Ministry of the Interior) – Micro Systemation, A.B. – May 9-13, 2016, London, UK.

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Feb 22-26, 2016, Jakarta, Indonesia.

Mobile Device Forensics Consultation, U.S. Department of State ATA, Feb 8-19, 2016, Jakarta, Indonesia.

Foundation & Kiosk XRY Mobile Phone Forensics - Micro Systemation, A.B. – Feb 2-4, 2016 – Singapore

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Oct 21-25, 2015 – Washington, DC

Proactive Internet Investigations Course - U.S. Department of State ATA – Aug 10 - 21, 2015 – Mexico City, Mexico

EnCase Transition Training, Bunting Digital Forensics Custom Course, May 26 – 27, 2015 Delaware State Police Child Predator Task Force, Dover, DE

Foundation and Intermediate XRY Mobile Phone Forensics (private course for 5 members of the Kingdom of Saudi Arabia Ministry of the Interior) – Micro Systemation, A.B. – May 18-22, 2015 – New York, NY

Introduction to Digital Forensics and Investigation - U.S. Department of State ATA, May 3 - 14, 2015, Muscat, Oman

EnCase I (Guidance Software Course - ATP) – Abu Dhabi Police Department – Mar 1 – Mar 5, 2015 – Abu Dhabi, United Arab Emirates

Proactive Internet Investigations Course - U.S. Department of State ATA – Jan 26 - Feb 6, 2015 – Cuernavaca, Mexico

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – Jan 16-23, 2015 – Cuernavaca, Mexico

Proactive Internet Investigations Course - U.S. Department of State ATA – Nov 17 - 28, 2014 – Tijuana, Mexico

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – Nov 6-14, 2014 – Tijuana, Mexico

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Oct 20-24, 2014 – Alexandria, VA

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Sep 22-26, 2014 – Santiago, Chile

Proactive Internet Investigations Course – U.S. Department of State ATA – August 11 – 22, 2014 – Ciudad de México, México

Digital Forensic Lab Mentoring and Consulting – Lead Instructor - U.S. Department of State ATA, July 14 – 25, 2014, Medellin & Bucaramanga, Colombia

Cyber Security Investigations: Incident Response – U.S. Department of State FedCTE Program – June 24, 2014, Virtual Class - AvayaLive

Digital Forensic Lab Mentoring and Consulting – Lead Instructor U.S. Department of State ATA, May 5 – 16, 2014, Cali & Pereira, Colombia

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, Mar 24 – Apr 4, 2014, Bogota, Colombia

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Apr 7-11, 2014 – Alexandria, VA

Foundation and Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Mar 3-7, 2014 – Vancouver, BC

Proactive Internet Investigations Course - Lead Instructor - U.S. Department of State ATA – Jan 27 – Feb 7, 2014 – Ciudad Juarez, Mexico

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – Jan 20-25, 2014
– Ciudad Juarez, Mexico

Intermediate XRY Mobile Phone Forensics – Micro Systemation, A.B. – Nov 20-22, 2013 –
San Diego, CA

Identification & Seizure of Digital Evidence - U.S. Department of State ATA – Nov 4-9, 2013 –
Chihuahua, Mexico

Computer Forensics for Legal Professionals, September 24, 2013, Widener University School
of Law, Wilmington, DE

Introduction to Digital Forensics and Investigation - Lead Instructor - U.S. Department of
State ATA, September 2-13, 2013, Mexico City, Mexico

Digital Forensic Lab Mentoring and Consulting - U.S. Department of State ATA, July 15-26,
2013, Dakar, Senegal

Introduction to Digital Forensics and Investigation (New Version Pilot) - Lead Instructor -
U.S. Department of State ATA, April 8-19, 2013, Manila, Philippines

Identification & Seizure of Digital Evidence - Lead Instructor - U.S. Department of State ATA
– Mar 9-17, 2013 – Muscat, Oman

Identification & Seizure of Digital Evidence - U.S. Department of State ATA - Feb 11-21, 2013
- Dakar, Senegal

Mastering Macintosh Forensics, Alvarez & Marsal, Oct 29 - Nov 2, 2012, 2012, Washington,
DC

Incident Response Tabletop Exercise, large web hosting client, Oct 16-17, 2012, San Antonio,
TX

Macintosh Incident Response, HTCIA, Sept 16-19, 2012, Hershey, PA

Windows Server Incident Response - Lead Instructor - Organization of American States, Sept
3-7, 2012, Trinidad & Tobago

Fundamentals of Network Security, U.S. Department of State ATA, July 23 - Aug 3, 2012,
Bogota, Colombia

Introduction to Digital Forensics and Investigation (Pilot for revised program) - U.S.
Department of State ATA, April 23 - May 4, 2012, Mexico City, Mexico

Mastering Macintosh Forensics, Ocean County Prosecutor's Office, April 16-20, 2012, Tom's
River, NJ

Advanced Digital Forensics Consultation (Windows / Linux / Macintosh Server Incident Response), Developer and Lead Instructor - U.S. Department of State ATA Mar 5-16, 2012, Bogota, Colombia

Cyber Unit Management Consultation, U.S. Department of State ATA, Sept 5-16, 2011, Bogota, Colombia

Cell Phone Forensics Consultation, U.S. Department of State ATA, July 11-22, 2011, Antigua.

Macintosh Forensics & Advanced Forensics Consultation, Developer and Lead Instructor - U.S. Department of State ATA, June 6-17, 2011, Bogota, Colombia.

Forensic Equipment Grant Consultation, U.S. Department of State ATA, May 17-31, 2011, Bangkok, Thailand

Introduction to Digital Forensics and Investigation - U.S. Department of State ATA, May 2-13, 2011, Mauritius

Advanced Forensic Acquisition & Analysis - Delaware ICAC - March 21-25, 2011, Dover, DE

Forensic Acquisition & Analysis - Delaware ICAC- Feb 21-25, 2011, Dover, DE

Cyberbullying - Cape Henlopen High School - January 27, 2011, Lewes, DE

Software Consultation: EnCase 1 & EnCase 2, U.S. Department of State ATA, Jan 10-21, 2011, Bangkok, Thailand

Incident Response & Forensic Tools Overview - Delaware Cyber Terrorism Exercise, Oct 27, 2010, Smyrna, DE

Identification & Seizure of Digital Evidence - U.S. Department of State ATA - June 3 - 11, 2010 - Mexico City, MX

EnCase Computer Forensics I – Lead Instructor - North Carolina ICAC- April 26 - 30, 2010 - Raleigh - Durham, NC

EnCase Computer Forensics II – Lead Instructor - Sidley Austin LLP - February 22 - 25, 2010 - Chicago, IL

EnCase Computer Forensics I - Qatar National Bank - October 11 - 15, 2009 - Doha, Qatar

EnCase Computer Forensics I - Abu Dhabi Police Department - October 4 - 8, 2009 - Abu Dhabi, UAE

Introduction to Computer Forensics - University of Delaware Police - August 17-21, 2009 - Lewes, DE

Advanced Computer Forensics Techniques - Computer Forensics Analysis and Training Center - June 4-5, 2009 - Sharon Hill, PA.

Cyberbullying - May 11, 2009 - Long Neck Elementary School - Millsboro, DE

"Computer Forensics - Current State and Future Challenges" - Computer Crimes Colloquium - April 7, 2009 - Wilmington University - Dover, DE

Identity Theft - City of Lewes Neighborhood Watch Meeting - March 23, 2009 - Lewes, DE

Disaster Recovery (CIS 486) - Goldey-Beacom College - January to March 2008 - Wilmington, DE.

Forensic Acquisition and Analysis - November 16-20, 2008, Dubai Police Department, Dubai, UAE

Cyber Stalking - Delaware Domestic Violence Council - Dover Police Department, November 7, 2008, Dover, DE

Computer Forensics (CIS 362) - Goldey-Beacom College - October to December 2008 - Wilmington, DE.

Advanced Computer Forensics - September 22-26, 2008, Sidley - Austin in Chicago, IL

Computer Forensics Primer for the Press - September 17, 2008 - Delaware Valley Press Club - Chester, PA.

Investigation Crimes Involving Computers - August 28-29, 2008 - Newark, DE.

Introduction to Computer Forensics - Computer Forensics and Analysis Training Center - August 26-27, 2008 - Sharon Hill, PA.

Disaster Recovery (CIS 486) - Goldey-Beacom College - March to April 2008 - Wilmington, DE.

Computer Forensics (CIS 362) - Goldey-Beacom College - October to December 2007 - Wilmington, DE.

Computer Forensics for Medical / Legal Professionals - University of Delaware Special Programs - November 9, 2007

Windows Network Investigations and Forensics - HTCIA Regional Training - June 19, 2007 - Newark, DE

User Services - First Response to Crime Scenes Workshop - Special Interest Group on University and College Computing Services - Edmonton, Canada - November 5, 2006

Cyber Stalking - Delaware Domestic Violence Council - November 16, 2006 - Dover, DE.

Computer Forensics for Prosecutors - Delaware Attorney General Staff - September 28, 2006 - Dewey Beach, DE.

CyberSpeak Podcast - Microsoft Log Parser Forensic Applications - June 3, 2006

CyberSpeak Podcast - User Assist Registry Key and Restore Point Forensics - May 13, 2006

Investigation of Cyber Incidents - University of Delaware System Administrators Group - May 17, 2006 - Newark, DE

Identity Theft and Cyber Safety - DuPont Experimental Station Staff - March 14, 2006 - Wilmington, DE.

Computer Forensics for Prosecutors - Delaware Attorney General Staff - September 22, 2005 - Lewes, DE.

First Response Issues for Crimes Involving Computers - Hosted by the U.S. Attorney's Office - September 16, 2005 - Dover, DE.

Examination of Photoshop Layer Data - RCFG GMU 2005 - August 15 & 18, 2005 - Fairfax, VA

Cyber-sabotage, Espionage, & Other Security Threats, February 23, 2005, Lorman Education Services, Newark, DE

Computer Forensics in the Courtroom, January 7, 2005, Widener University School of Law, Wilmington, DE

Computer Forensics for Prosecutors - Delaware Attorney General Staff - September 30 - October 1, 2004 - Dewey Beach, DE.

Forensic Examination of Peer-to-Peer Client Software Artifacts -NJSP High Tech Crime Unit. September 22, 2004, Trenton, NJ.

Introductory Computer Forensics Guidance Software - Sterling, VA Jun 29 - Jul 2, 2004 (32 hrs) Lead Instructor

Internet / Email Examinations Guidance Software - Sterling, VA Jun 22 - 25, 2004 (32 hrs) Lead Instructor

Email Examinations Lab at CEIC 2004 Myrtle Beach, SC Jun 6 - 9, 2004 (7.5 hrs - five presentations) Lead Instructor

Photoshop Layer Metadata Examinations CEIC 2004 Myrtle Beach, SC Jun 8, 2004 (1.5 hrs) Lead Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Apr 27 - 30, 2004 (32 hrs) Lead Instructor

Internet / Email Examinations Guidance Software - Sterling, VA Mar 30 - Apr 2, 2004 (32 hrs) Instructor

Internet / Email Examinations Guidance Software - Sterling, VA Feb 3-6, 2004 (32 hrs) Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Jan 6-9, 2004 (32 hrs)
Lead Instructor

Internet / Email Examinations Guidance Software - Sterling, VA Nov 18-21, 2003 (32 hrs)
Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Oct 21-24, 2003 (32 hrs)
Instructor

Intermediate Analysis & Reporting Guidance Software - Sterling, VA Sept 9-12, 2003 (32 hrs)
Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Aug 12-15, 2003 (32 hrs)
Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA July 8-11, 2003 (32 hrs)
Instructor

Intermediate Analysis & Reporting Guidance Software - Sterling, VA June 17-20, 2003 (32 hrs)
Instructor

Internet / Email Guidance Software - Sterling, VA May 6-9, 2003 (32 hrs) Instructor

Intermediate Analysis & Reporting Guidance Software - Sterling, VA Mar 4-7, 2003 (32 hrs)
Instructor

Introductory Computer Forensics Guidance Software - Sterling, VA Feb 25-28, 2003 (32 hrs)
Instructor

Internet Safety for Children - Winter / Spring 2003 semester offering through the University of Delaware Continuing Education Division

Cyber-Stalking and Related Crimes Involving Computers: October 7, 2002 in Newark, DE.

Computer Crime Issues for Prosecutors: - Presented to the Wicomico County States Attorney's Office (4/20/01) and to the Attorney General's Office for the State of Delaware Sex Crimes Unit (10/4/02).

Computer Forensics: - during the spring semester 2002, supervised and directed an independent course of study in computer forensics for a University of Delaware senior majoring in computer science. Program was under the auspices of Professor Chien-Chung Shen. Student is now employed with Price, Waterhouse, Cooper in the computer forensics division.

The Internet as an Investigative Tool: Presented at the University of Delaware (5 presentations: 12/5/00, 1/8/01, 8/6/01, 8/13/01, & 8/26-27/02), at the Eastern Shore Criminal Justice Academy (3 presentations: 2/16/01, 3/8/01, and 3/20/01), and at Mount St. Mary's College (6/26/02).

Computer Crimes: 1st Responder Issues - course developed and presented to the University of Delaware Police as a 2-hour block during in-service training. Presented May 31, 2001, June 7, 2001, May 30, 2002, and June 5, 2002.

Training Courses Completed

AX300 – AXIOM Advanced Mobile Examinations	Magnet Forensics – Oct 24–27, 2017 Sterling, VA
iVE Vehicle Forensics	Berla – Sep 25–29, 2017 Annapolis, MD
AX200 - AXIOM Examinations	Magnet Forensics – Sep 19–22, 2017 Online
XRY Train-the-Trainer Training	MSAB – Aug 30– Sep 1, 2017 Stockholm, SE
XRY Version 7 Training	MSAB – Aug 22–26, 2016 Stockholm, Sweden
XRY Version 7 Training	MSAB – Mar 28–Apr 1, 2016 Stockholm, Sweden
XRY Advanced Acquisitions	MSAB – Mar 21 – 25, 2016 Freehold, NJ
XRY Advanced Applications Analysis	MSAB – Dec 14 – 18, 2015 Washington, DC
XRY Train-the-Trainer Annual Training	MSAB – Sept 7–11, 2015 Stockholm, Sweden
XRY Train-the-Trainer Course	MSAB – Sept 30– Oct 11, 2013 Stockholm, Sweden
FTK Bootcamp Version 3	Access Data - April 5–7, 2011 - Online
XRY Physical Acquisition & Analysis Training	MSAB - Oct 6–8, 2010 - Alexandria, VA
XRY Logical Acquisition & Analysis Training	MSAB - Oct 4–5, 2010 - Alexandria, VA
Basic Malware Analysis	HB Gary - April 20–21, 2010 - Columbia, MD
LAW PreDiscovery Certified Administrator Course	LexisNexis - Jan 14, 2010 - Washington, D.C.
LAW PreDiscovery EDD Certified User Course	LexisNexis - Jan 12–13, 2010 - Washington, D.C
Microsoft Exchange Server 2007	Global Knowledge - Jan 26 - 30, 2009 - Arlington, VA
HTCIA Conference (24 hrs)	High Tech Crime Investigator's Association - Oct 20–22, 2008, Atlantic City, NJ
Neutrino Cell Phone Forensics (16 hrs)	Guidance Software - January 15 – 16, 2008, Sterling, VA.
Macintosh Forensics (40 hrs)	Phoenix Data Group - October 15–19, 2007 - Sharon Hill, PA

Vista Forensics	Access Data - July 20, 2007 - Washington, DC
Advanced Windows Intrusion Investigator's Course (40 hrs)	SYTEX - February 27 – March 3, 2006, FBI Academy, Quantico, VA
Adobe Photoshop for Forensic Video Analysts (16 hrs)	Resolution Video - December 14-15, 2005 - Reston, VA
Regional Computer Forensics Group Seminar (40 hrs)	RCFG / HTCIA - August 15-19, 2005 - GMU - Fairfax, VA.
Cell Seizure (16 hrs)	Paraben - May 18-19, 2005 in Newark, DE
PDA Seizure (16 hrs)	Paraben - May 16-17, 2005 in Newark, DE
Enterprise Security & Vulnerability (36 hrs)	USSS / SEARCH - April 18-22, 2005 in Cherry Hill, NJ
Access Data FTK Advanced Internet Training Course (24 hrs)	Access Data - March 15 – 17, 2005 in Dover, DE.
Ocean Systems: dTective (Advanced Video Forensic Analysis) (16 hrs)	Ocean Systems - Feb. 24 – 25, 2005 in Burtonsville, MD.
Advanced UNIX Investigator's Course (40 hrs)	SYTEX - December 6 – 10, 2004, Ellicott City, MD.
EnCase EnScript Programming (32 hrs)	Guidance Software - November 16 – 19, 2004, Sterling, VA.
Networks and Networking for Agents / System Security and Exploitation (80 hrs)	SYTEX - October 18 – 29, 2004, Ellicott City, MD.
Law Enforcement Video Association Annual Training Conference 2004 (16 hrs)	LEVA - October 6 – 7, 2004 Washington, D.C.
NIJ Law Enforcement Technology Institute 2004 (40 hrs)	NIJ - July 11 – 16, 2004, Washington, D.C.
Computer and Enterprise Investigations Conference / TechnoSecurity Conference 2004 (28 hrs)	Guidance Software - June 6 – 9, 2004 in Myrtle Beach, SC.
Ocean Systems: dTective (Advanced Video Forensic Analysis) (16 hrs)	Ocean Systems - May 6 – 7, 2004 in Burtonsville, MD.
Ocean Systems: Introduction to Forensic Video Examinations (24 hrs)	Ocean Systems - May 3 – 5, 2004 in Burtonsville, MD.

Access Data FTK Intermediate Training Course (24 hrs)	Access Data - April 5 – 7, 2004 in Dover, DE.
EnCase Expert Series: Internet & Email Examinations (32 hrs)	Guidance Software - February 4 - 7, 2003 in Sterling, VA.
EnCase Advanced Computer Forensics (32 hrs)	Guidance Software - January 21- 24, 2002 in Sterling, VA.
Introduction to Programming Concepts (Visual Basic 6) (50 hrs)	University of Delaware Course - Wilm, DE – Fall 2002
Computer and Enterprise Investigations Conference 2002 (16 hrs)	Guidance Software - September 16-17, 2002 Chantilly, VA.
Regional Computer Forensics Group Seminar (40 hrs)	RCFG / HTCIA - August 12-16, 2002 - GMU - Fairfax, VA.
ILook Computer Forensics Software (24 hrs)	ACES / FBI / IRS / NCFS - July 23-25, 2002 Orlando, FL.
Firewalls and Virtual Private Networks (16 hrs)	CSI / NIPC / FBI - May 22-23, 2002 MSP - Columbia, MD.
Internet Investigations and Child Exploitation Overview (8 hrs)	SEARCH - April 6, 2002, CCU - Conway, SC.
Techno-Security 2002 Conference (28 hrs)	The Training Company - April 7-10, 2002 - Myrtle Beach, SC
Enterprise Networks (50 hrs)	University of Delaware - Wilm, DE - Spring 2002
EnCase Advanced Computer Forensics (32 hrs)	Guidance Software - February 19-22, 2002 - Leesburg, VA.
LAN (Local Area Networks) (50 hrs)	University of Delaware - Newark, DE - Fall 2001
EnCase Intermediate Computer Forensics (32 hrs)	Guidance Software - August 7-10, 2001 - Leesburg, VA .
Techno-Security 2001 Conference (28 hrs)	The Training Company April 22-25, 2001 - Myrtle Beach, SC
WAN (Wide Area Networks) (50 hrs)	University of Delaware - Newark, DE - Spring 2001

Advanced Data Recovery and Analysis Course (40 hrs)	NW3C - October 23-27, 2000 - Fairmont, WV.
The Internet as in Investigative Tool (8 hrs)	NW3C / IFCC - October 12, 2000 - Fairmont, WV.
Basic Data Recovery and Analysis Course (40 hrs)	NW3C July 24-28, 2000 in Myrtle Beach, SC.

Computer Forensics Expert Witness Experience

Crawford and Company v Larry W. Daniel and Cunningham Lindsey Claims Management, Inc Civil Case No 17-1-01244 – Superior Court of Cobb County State of Georgia – Submitted affidavit on September 12, 2017 on behalf of Crawford that an iPhone submitted by the defendant as part of electronic discovery had the messages set to delete after 30 days and that the user has enabled backup encryption, thereby preventing the contents from being acquired. Case settled without going to trial.

AdMarketer, LLC and Credit Benefit Services, LLC v Isaac “Zack” Bernato; Dennis H. James; CRM Holding Company, LLC; IMT Marketplace, LLC; World Clicks, LLC; and Valerie DiNardo – Civil Action File No: 2015CV267337 in the Superior Court of Fulton County State of Georgia – Submitted affidavit on March 31, 2017 on behalf of the defendant that opposing expert had made a finding that defendant had deleted messages, thus supporting a spoliation claim. Affidavit stated that opposing expert had not discovered iPhone message setting for ‘delete after 30 days’ nor had he discovered that SMS forwarding was enabled, enabled specifically to a Mac laptop that was in the possession of the opposing expert and which opposing expert had failed to examine. This laptop contained all the chat messages that the expert claimed were deleted. Further the affidavit stated that the opposing expert had used only one tool in his examination and in doing so missed over 11,000 AIM messages, many of which were relevant to the case. Defendants filed bankruptcy and case settled without trial.

Tamika Covington vs International Association of Approved Basketball Officials, Board 193, et al. (CIVIL ACTION NO. 3:08-cv-03639) - US District Court (Princeton, NJ) – Testified as expert for defense in computer forensics analysis and email analysis in a hearing to dismiss based on fraudulent documents offered into evidence by plaintiff. Specifically, testified that document proffered as an email was in fact fabricated to appear as such. – July 09, 2014.

Network Computing Services Corporation vs Haynsworth, Sinkler, P.A. Belton T. Zeigler and John Tiller (South Carolina) – Submitted two affidavits for the plaintiff regarding deleted emails in a case alleging legal malpractice – April 2010

State of Delaware vs Irina Malinovskaya (3rd trial - Murder 1st) – Testified as computer forensics expert regarding analysis of defendant’s computer. Also testified that an email offered by the defendant after the 2nd trial was fabricated and offered as evidence. The defendant was convicted of tampering with physical evidence. - 2007

Cpl B. Kurt Price et al. vs Colonel L. Aaron Chaffinch et al. (US District Court) Submitted affidavit as to wiping of a hard drive by the plaintiff - May 2006

State of Delaware vs Irina Malinovskaya (2nd trial - Murder 1st) Testified - 2006

State of Delaware vs Stephanie McMullen (Munchausen's Nurse case) Testified - 2006

State of Delaware vs Eric Kemske (Manufacture, distribute, possess child pornography – peer-to-peer software involved) – Testified - 2005

State of Delaware vs Keith Appleby (Suppression Hearing - Computer Intrusion Case) Testified - 2003